



U.S. Department of Justice

Antitrust Division

*Liberty Square Building
450 5th Street, N.W.
Washington, DC 20530*

September 20, 2024

VIA ECF

Honorable Leda Dunn Wettre, U.S.M.J.
U.S. District Court for the District of New Jersey
Martin Luther King Jr. Bldg. & U.S. Courthouse
50 Walnut Street
Newark, New Jersey 07102

**Re: *United States of America, et al. v. Apple Inc.*, No. 2:24-cv-04055 (JXN-LDW)
Joint Letter Regarding Disputes Over the Protective Order, ESI Protocol,
and Source Code Protocol**

Dear Judge Wettre:

Plaintiffs and Defendant respectfully submit this joint letter pursuant to the Court's Order dated August 7, 2024 (ECF No. 94). The parties have met and conferred on numerous occasions since the issuance of the Order and over the previous several months. This letter outlines the areas of dispute over the Protective Order, ESI Protocol, and Source Code Protocol. Accompanying this letter are Plaintiffs' and Defendant's proposed Protective Orders (Exhibits A and B, respectively), the proposed ESI Protocol with Plaintiffs' and Defendants' separate positions identified (Exhibit C), and the proposed Source Code Protocol with Plaintiffs' and Defendants' separate positions identified (Exhibit D).

I. GLOBAL ISSUE (Definition of "Party" and "Parties")¹

A. Plaintiffs' Position

The Antitrust Division of the U.S. Department of Justice and the respective Attorneys General of the Plaintiff States initiated this antitrust enforcement action as plaintiff prosecutors. Consistent with this prosecutorial role, in these discovery-related protocols, Plaintiffs define the "Parties" as "the Antitrust Division of the United States Department of Justice, the Attorney

¹ The issue concerning the definition of "Parties" applies to all three protocols. It is the only matter in dispute on the Data Source Code Protocol. *See* Ex. D §2(n).

Generals for the Plaintiff States, and Defendant.”² Apple insists that the parties for purposes of these orders means “the United States” as a whole and “the Plaintiff States” as a whole. For these discovery protocols, the Court should adopt Plaintiffs’ definition as commensurate with the actual scope of Plaintiffs’ preservation and discovery obligations in this case.

Apple’s position—that it is entitled to seek “party” discovery from potentially every federal and every state agency—is unfounded, premature, and unduly burdensome. Apple offers no justification for why extensive party discovery of hundreds of federal and state agencies is relevant and proportional to the needs of the case, why non-party discovery would not suffice, or how any potential evidentiary value would justify the burden involved. Nor can it, because Apple fails to identify any particular federal or state agency from whom it may seek discovery or the concrete nature and scope of such discovery.³

1. Party Discovery Obligations Do Not Extend to the Entirety of Government

The Federal Rules, case law, and common sense dictate that discovery obligations do not extend to the entirety of a government every time a prosecuting agency files suit. The Federal Rules limit party discovery to materials in the parties’ “possession, custody, or control.” FED.R.CIV.P. 34(a)(1). In civil cases brought by the federal government, courts routinely conclude that materials in the “possession, custody, or control” of the United States are limited to the prosecution team and any agencies that jointly participated in, or significantly contributed to, the case:

The United States acting as plaintiff prosecutor does not open up the entire federal government to party discovery. . . . Rather, the custody or control of discoverable materials extends to the materials in possession of the federal agency that is engaged in a joint or combined effort to prosecute a matter.

United States v. Xlear Inc., 2022 WL 5246717, at *2 (D. Utah Oct. 6, 2022) (cleaned up); *Deane v. Dynasplint Sys., Inc.*, 2015 WL 1638022 at *4 (E.D. La. Apr. 13, 2015) (collecting more than a dozen cases explaining that discovery extends to another agency only “when the Justice Department is engaged in a joint effort with that other agency or when the other agency is so closely aligned with the Justice Department as to be part of the prosecuting government team or has contributed significantly to the investigation or prosecution”). Criminal cases similarly limit party discovery against the United States to materials in the possession, custody, and control of the prosecution team. *United States v. Cano*, 934 F.3d 1002, 1023 (9th Cir. 2019) (“[A] federal prosecutor need not comb the files of every federal agency”).

² Ex. A, §A.2.1; Ex. C §1.8; Ex. D §2(n).

³ Discovery has not been commenced. Should the scope of Party discovery arise in the context of contested discovery requests, Plaintiffs will fully brief the issue.

The proposals before the Court—especially the ESI Protocol—impose broad-based discovery obligations on the “Parties.” The ESI Protocol requires “[e]ach Party” to “preserve potentially relevant and discoverable Documents and ESI,” including text messages, voicemails, video files, and documents in collaborative platforms. These obligations properly encompass the U.S. Department of Justice’s Antitrust Division and the State Antitrust Divisions of the Offices of the Attorney General for the twenty Plaintiff States.⁴ But these obligations do not extend to the NASA, the Library of Congress, or the hundreds of other federal agencies that are not prosecuting this action. Nor do these obligations cover state agencies like the fifty-plus New Jersey State agencies besides its prosecutor.

2. Apple’s Caselaw Is Unavailing

Apple leans on *United States v. American Telephone & Telegraph Co.* in its bid for whole-of-government discovery. 461 F. Supp. 1314 (D.D.C. 1978) (“*AT&T*”). But *AT&T* is limited to its “peculiar facts,” *id.* at 1334, which are not present here. In *AT&T*, “the nature and extent of the [federal] regulation to which defendants are subject” and the “Government’s own policies” were squarely at issue, because the prosecutors had coordinated with “government executives involved in economic policy,” “the White House,” and “various [other] government departments.” *Id.* For those reasons, the court concluded that the case was “likely to involve the documents and the activities of a great number of government departments” and therefore a broad definition of “Plaintiff” fit the needs of the case. *Id.* Mindful that the ruling “might encourage other litigants in other cases to rummage through the files of the entire government, and so paralyze both the work of numerous agencies and that of the courts,” the court limited its holding to “these peculiar facts.” *Id.*

Those facts are not present here. This case does not involve a cross-agency investigative effort or implicate the records of many government agencies. There are no specific federal agencies or employees on the Parties’ initial disclosures. And, here, as in *AT&T*, authorizing party discovery on the entire government would risk grave adverse consequences.

Similarly, the Attorneys General brought this action in their independent law enforcement capacity representing the people of their states. They are neither seeking relief for state agencies nor asserting damages claims. Numerous courts conclude that state agencies “are not to be treated as parties to [an] action for the purposes of discovery.” See *Colorado v. Warner Chilcott Holdings Co. III*, 2007 WL 9813287, at *4 (D.D.C. May 8, 2007) (“[W]here two government agencies are neither interrelated nor subject to common executive control, they will not be aggregated together for purposes of discovery.”); *United States v. Am. Express Co.*, 2011 WL 13073683, at *2 (E.D.N.Y. July 29, 2011) (“[T]he decision to pursue an enforcement action against Amex was one of policy, made independently of the State Governors and state agencies. . . . for purposes of this litigation and discovery, the state agencies [with one exception] are not parties”); *United States v. Novartis Pharms. Corp.*, 2014 WL 6655703, at *9 (S.D.N.Y. Nov. 24, 2014) (“[T]he mere fact

⁴ The “State Antitrust Divisions” are the units, departments, or subdivisions within the Offices of the Attorney General of each respective Plaintiff State that are responsible for enforcing the laws and claims asserted in this litigation.

that a state or a state agency sues does not mean that the records of all state agencies may be discovered using Rule 34's tools."). Apple's definition of "Party" is neither appropriate nor proportional.

B. Defendant's Position

Plaintiffs' proposed definition of "Party" would dramatically and unjustifiably narrow the scope of Plaintiffs' discovery obligations. Apple seeks to define "Party" or "Parties"—quite naturally—as the parties to this lawsuit—that is, "any individual Plaintiff or the Defendant in the above captioned action." *See* Dkt. 51. That would define the term "Parties" to include the United States of America, each of the Plaintiff States, and Apple Inc. Apple's definition is consistent with both common sense and how the term "Party" has been defined in similar discovery protocols in government antitrust cases. *See, e.g., FTC v. Amazon.com, Inc.*, No. 2:23-cv-01495-JHC, Dkt. 160 at § 2.11 (W.D. Wash. Feb. 13, 2024); *Texas v. Google LLC*, No. 4:20-cv-00957-SDJ, Dkt. 101 at 5 (E.D. Tex. Apr. 14, 2021); *United States v. UnitedHealth Grp., Inc.*, No. 1:22-cv-00481 (CJN), Dkt. 28 at 3 (D.D.C. Mar. 9, 2022); *United States v. Visa Inc.*, No. 4:20-cv-07810-JSW, Dkt. 49 at 3 (N.D. Cal. Nov. 25, 2020).

Plaintiffs rejected that straightforward definition. Instead, Plaintiffs insist on defining "Parties" to include *only* "the Antitrust Division of the United States' Department of Justice, the Attorneys General for the Plaintiff States, and Defendant in this Action." That makes no sense. Neither the Antitrust Division nor any state attorney general is a named plaintiff in this case. Rather, they are merely divisions of governmental agencies tasked by the United States and Plaintiff States with litigating this case. Insisting that the Plaintiff parties be limited in this way is akin to Apple insisting that the term "Defendant" include only the law firms or in-house counsel representing Apple in this case. Such a construction is illogical, and the Court should reject it. The term "Parties" should be defined by the entities named in the caption—no more, no less.

Plaintiffs' efforts to artificially limit the scope of who constitutes a "Party" appears driven by their desire to restrict the scope of their discovery obligations. Apple intends to seek discovery from the various federal and state agencies that have relevant information. Because the United States and Plaintiff States are named parties, Apple will serve those requests as "party" discovery. Apparently anticipating that, Plaintiffs seek to define the term "Party" narrowly to avoid obligations to preserve, collect, review, and produce documents from various federal and state agencies.

That effort runs aground on common sense and ample precedent. *United States v. Am. Tel. & Tel. Co.* addressed this same question: "who is the plaintiff?" 461 F. Supp. 1314, 1330 (D.D.C. 1978). There, the United States argued that "plaintiff" meant only the Department of Justice and that all other agencies and governmental departments were not parties and, therefore, subject only to third-party discovery under Federal Rule of Civil Procedure 45. *Id.* In rejecting the government's position, the court recognized that "th[e] action, as its caption indicates, was brought not on behalf of the Department of Justice but on behalf of the United States of America." *Id.* at 1333. Particularly in the context of an antitrust case that was "national in scope," involved "broad economic policy," and was likely to implicate "the documents and the activities of a great number of government departments," the court noted that "it simply ma[de] no sense to hold that the Department of Justice, which essentially is a law office, alone comprises the United States." *Id.*

at 1333-34. Thus, the court held that “the United States, having filed the action, cannot claim to be merely the Department of Justice.” *Id.* at 1334; *see also United States v. Atrium Village Assocs.*, 1988 WL 2778, at *1 (N.D. Ill. Jan. 12, 1988) (“[A] fair reading of [AT&T] is that it is unrealistic to view the Department of Justice as the sole plaintiff when the United States brings a federal law enforcement action.”); *North Dakota v. United States*, 2021 WL 6278456, at *4-6 (D.N.D. Mar. 24, 2021) (noting that “the United States’ obligation to respond to discovery requests is not limited to an agency named in the action” and that North Dakota was not foreclosed “from seeking discovery from other federal agencies who possess relevant information” under Rule 34).⁵

The same is true for state attorneys general bringing cases on behalf of their states. *See Washington v. GEO Grp., Inc.*, 2018 WL 9457998, at *3 (W.D. Wash. Oct. 2, 2018) (“[W]here the plaintiff is the State of Washington, discovery addressed to the State of Washington includes its agencies. Because the [Attorney General’s Office] is the law firm of the State of Washington, [it] should respond to and produce discovery on behalf of the State of Washington, including its agencies.”). Plaintiff States cannot avoid their obligations to preserve and produce relevant documents from state agencies through narrow wordsmithing. *Cf. In re Generic Pharms. Pricing Antitrust Litig.*, 699 F. Supp. 3d 352, 357-61 (E.D. Pa. 2023) (ordering several state attorneys general to produce documents from other state agencies under Rule 34 in a “wide-ranging” antitrust lawsuit); *In re Social Media Adolescent Addiction/Personal Injury Prods. Liability Litig.*, 2024 WL 4125618, at *24-129 (N.D. Cal. Sept. 6, 2024) (granting Meta’s motion to compel production of state-agency documents under Rule 34 from thirty-four plaintiff states involved).

Plaintiffs brought this case on behalf of the United States and each of the Plaintiff States. Plaintiffs must now carry the discovery and preservation obligations that go along with naming those entities as parties to the litigation.

II. PROTECTIVE ORDER

A. Plaintiffs’ Position

Plaintiffs’ Proposed Protective Order (“PPO”): (1) provides for one category of designation, Confidential, where Confidential Information could be disclosed only to four

⁵ Plaintiffs’ cases are not to the contrary. In *Deane v. Dynasplint Sys., Inc.*, a civil case alleging illegal Medicare reimbursements, each of the “more than a dozen cases” cited by the court were criminal cases, *see* 2015 WL 1638022, at *4 (E.D. La. Apr. 13, 2015), where discovery rules are more limited. Far from definitively limiting party discovery to the prosecuting agency, the court opined that “the scope of the government’s obligation to produce documents ... turn[s] on the extent to which the prosecutor has knowledge of and access to the documents.” *Deane*, 2015 WL 1638022, at *4 (quoting *United States v. Libby*, 429 F. Supp. 2d 1, 6 (D.D.C. 2006)). The court held that for purposes of party discovery, the parties included not only the Department of Justice and U.S. Attorney’s Office, but also the Department of Health and Human Services and Centers for Medicare & Medicaid Services. *Id.* at *5. Similarly, in *United States v. Xlear Inc.*, the court noted that obtaining agency discovery through a government plaintiff can be appropriate for “[p]racticality reasons” where “Rule 45 subpoenas would ‘likely be more time-consuming and could result in delay of the litigation.’” 2022 WL 5246717, at *2 (D. Utah Oct. 6, 2022) (quoting *North Dakota*, 2021 WL 6278456, at *5)).

designated Apple In-House Attorneys who are identified to Plaintiffs and not involved in business decisions; (2) precludes disclosure to Apple non-lawyer officers, directors, or employees; and (3) requires a Receiving Party to comply with applicable data security and breach response notification laws and practices, consistent with prior antitrust litigation involving the United States and Plaintiff States. Apple's proposal essentially renders Confidential Information non-confidential. Such information would be broadly shared with Apple's officers, directors, and employees, and all of Apple's in-house counsel—more than 500 attorneys. There would be no practical limits on their ability to use this information to participate in business decision-making that impacts Apple's customers and competitors. These provisions do not meaningfully protect non-parties' Confidential Information. In addition, Apple's data security and breach proposals impose onerous burdens on Plaintiffs that are inconsistent with prior practice.

Plaintiffs request that the Court allow non-parties fourteen days to submit their own positions concerning the disclosure of Confidential Information.

1. Disclosure to Defendant's In-House Attorneys (PPO § I.21.e)

a. Plaintiffs' Proposal Provides Meaningful Protection Against Disclosure of Non-Party Confidential Information to Apple's In-House Attorneys

After months of negotiations, less than two weeks before this filing, Apple changed its position to reject the parties' apparent agreement that Confidential Information would be limited to four Apple In-House Attorney disclosed to Plaintiffs and not involved in business decisions. Apple noted on September 10 that the distinctions between the persons to whom Confidential Information and Highly Confidential Information could be disclosed had largely collapsed. Plaintiffs agreed and revised Plaintiffs' PPO to provide for only a single designation, Confidential. Apple preserved a two-designation structure that allowed disclosure of Confidential Information to an unlimited number of its In-House Attorneys whether they participate in competitive decision-making or not. Plaintiffs reject this last-minute and ill-advised change.

Plaintiffs' PPO protects Confidential non-party information while allowing Apple's In-House Attorneys to assist in their client's defense. In reviewing protective orders, courts balance the risk of inadvertent disclosure of commercially sensitive information to competitors against the needs of the party seeking discovery to prosecute or to defend the case. *Brown Bag Software v. Symantec Corp.*, 960 F.2d 1465, 1470 (9th Cir. 1992). Courts grant in-house counsel access to confidential information only after determining that those recipients do not participate in competitive decision-making. *See F.T.C. v. Whole Foods Mkt.*, 2007 WL 2059741, at *2 (D.D.C. July 6, 2007) (summarizing *U.S. Steel Corp. v. United States*, 730 F.2d 1465 (Fed. Cir. 1984), which "would preclude access to information to anyone who was positioned to advise the client as to business decisions that the client would make regarding, for example, pricing, marketing, or design issues when that party granted access has seen how a competitor has made those decisions"). "The primary concern underlying the 'competitive decision-making test' is that confidential information will be used or disclosed inadvertently because of the lawyer's role in the client's business decisions." *United States v. AB Electrolux*, 139 F. Supp. 3d 390, 392 (D.D.C. 2015).

The potential harm to non-parties is real. During Plaintiffs’ pre-Complaint investigations, Apple’s customers and competitors produced competitively sensitive information, including contracts, business strategies and plans, presentations to executives, and internal financial projections, and more will be produced during discovery. Non-parties strongly oppose allowing Apple’s In-House Attorneys’ access to their Confidential Information, expressing alarm that they may inadvertently rely on their Confidential Information when advising Apple about business decisions.

Apple raised similar concerns in a recent government antitrust enforcement action against Google. Apple sought to “prevent disclosure of certain highly confidential Apple materials to in-house counsel for Google,” because Google was Apple’s competitor “in the development of mobile operating system software, app stores, and mobile devices,” and its agreements with Google were at issue in the case. Non-Party Apple Inc.’s Position Statement on Protective Order in *United States v. Google*, 1:20-cv-03010 (D.D.C. Nov. 20, 2020), ECF 47 at 2. Apple argued that disclosure of competitively sensitive information “would directly implicate future business dealings between Apple and Google, provide Google with a substantial advantage over Apple in negotiations, and potentially disadvantage competitor[s] ... that negotiate with Apple[.]” *Id.* The same is true here, where Apple is the defendant, and its customers and competitors are non-parties.

Courts credit these concerns, recognizing the inherent risk of permitting in-house counsel access to confidential information of customers or competitors. The risk of inadvertent disclosure is higher for in-house counsel than outside counsel because compartmentalization of protected information is “a feat beyond the compass of ordinary minds,” and an “individual cannot rid himself of the knowledge he has gained; he cannot perform a prefrontal lobotomy on himself....” *F.T.C. v. Advocate Health Care Network*, 162 F. Supp. 3d 666, 669-70 (N.D. Ill. Feb. 29, 2016). *See Sullivan Mktg. v. Valassis Commc’ns*, 1994 WL 177795, at *3 (S.D.N.Y. May 5, 1994); *F.T.C. v. Exxon Corp.*, 636 F.2d 1336, 1350 (D.C. Cir. 1980).

Apple makes no effort to limit disclosure to In-House Attorneys with no role in business decisions. Even a narrowed version of Apple’s proposal that would allow some subset of unnamed In-House Attorneys to access Confidential Information would not avoid the risk of harm to non-parties, as In-House Attorneys routinely move from legal to business roles.

b. Apple Has Not Shown Prejudice

Apple has not shown that it would suffer prejudice by the limitations Plaintiffs propose, much less that such prejudice outweighs any risk of inadvertent disclosure. *Autotech Techs. Ltd. P’ship v. Automationdirect.com, Inc.*, 237 F.R.D. 405, 406–14 (N.D. Ill. 2006); *Presidio Components, Inc. v. Am. Tech. Ceramics Corp.*, 546 F. Supp. 2d 951, 953 (S.D. Cal. 2008).

Disclosure to In-House Attorneys is not a legal or practical imperative, and antitrust cases frequently proceed with protective orders that are limited to outside counsel only. *United States v. Anthem*, 1:16-cv-01493 (D.D.C. Sep. 15, 2016), ECF 129 at 10-11; *United States v. US Airways*, 1:13-cv-01236 (D.D.C. Aug. 30, 2013), ECF 55 at 8-9; *United States v. BCBS of Michigan*, 2:10-cv-14155 (E.D. Mich. May 10, 2012), ECF 169 at 6-8; *United States v. Dean Foods*, 2:10-cv-59 (E.D. Wis. May 20, 2010), ECF 30 at 7-9. That Apple’s experienced outside antitrust counsel will

have access to all Confidential Information is sufficient. *Advoc. Heath Care Network*, 162 F. Supp. 3d at 674; *Blackbird Tech LCC v. Serv. Lighting & Elec. Supplies*, 2016 WL 2904592, at *5 (D. Del. May 18, 2016).

Plaintiffs’ proposal to allow access to Confidential Information to four In-House Attorneys who are not involved in business decisions safeguards Confidential Information and follows established precedent for protective orders in antitrust cases and this District’s model Confidentiality Order. *Whole Foods Mkt.*, 2007 WL 2059741, at *1; *AB Electrolux*, 139 F. Supp. 3d at 391; *Philips N. Am. v. Glob. Med. Imaging*, 343 F.R.D. 59, 61 (N.D. Ill. 2022); *United States v. Sungard Data Sys.*, 173 F. Supp. 2d 20, 21 (D.D.C. 2001); *Brown Bag Software*, 960 F.2d at 1471; *United States v. Aetna*, 2016 WL 8738421, at *1 (D.D.C. Sept. 14, 2016); *United States v. UnitedHealth Group*, 1:22-cv-00481 (D.D.C. Mar. 9, 2022), ECF 28 at 10-11.⁶

If the Court is inclined to establish two tiers, then the Highly Confidential designation should impose even greater restrictions, limiting disclosure to outside counsel only. *United States v. Google*, 1:20-cv-03010 (D.D.C. Jan. 21, 2021), ECF 98 at 13-17; *United States v. Sabre Corp.*, 19-cv-1548 (D. Del. Sep. 10, 2019), ECF 24 at 11-12 (entered ECF 26); *New York v. Deutsche Telekom AG*, 19-cv-05434 (S.D.N.Y. Aug. 14, 2019), ECF 185 at 12-14; *United States v. Bazaarvoice*, 13-cv-00133 (N.D. Cal. Mar. 4, 2013), ECF 35 at 12-13; *United States v. Am. Express Co.*, 10-cv-4496 (E.D.N.Y. Apr. 7, 2011), ECF 102 at 10-13. Apple itself made this request in the Google case, arguing, “There is substantial risk that disclosure of Apple’s highly confidential material to employees of Google, including in-house counsel, would result in material harm to Apple.” Non-Party Apple Inc.’s Position Statement on Protective Order in *United States v. Google*, 1:20-cv-03010 (D.D.C. Nov. 20, 2020), ECF 47 at 1.

2. Disclosure to Defendant’s Non-Lawyer Officers, Directors, or Employees (PPO § I.21.f)

Apple proposes disclosures of Confidential non-party information to “representatives of Apple who are officers, directors, or employees of Apple, as well as their immediate staff, to whom [Apple deems] such disclosure is reasonably necessary,” placing sensitive non-party information in the hands of Apple’s most senior decision-makers. Allowing these individuals unfettered access to Confidential Information—including “confidential research or commercial information”—is highly prejudicial to non-parties. The risk that such information may influence Apple’s decision-makers is severe when they have direct access to that information. These concerns are amplified here where Apple may use its market dominance to thwart or punish companies that produce competitively sensitive information.

Courts regularly enter protective orders that preclude broad disclosure to a defendant’s officers, directors, and employees in antitrust enforcement actions brought by the United States. See *United States v. Google*, 1:20-cv-03010 (D.D.C. Jan. 21, 2021), ECF 98 at 13-17; *United States v. JetBlue Airways*, 1:23-cv-10511 (D. Mass. Mar. 20, 2023), ECF 63-1 at 13-16 (entered ECF 65); *United States v. Assa Abloy*, 1:22-cv-02791 (D.D.C. Oct. 3, 2022), ECF 33 at 10-11; *United*

⁶ Apple’s same outside counsel at Kirkland & Ellis entered into the stipulated protective order on behalf of UnitedHealth.

States v. Booz Allen Hamilton Holding Corp., 1:22-cv-01603 (D. Md. July 18, 2022), ECF 71 at 9-11; *United States v. UnitedHealth Group*, 1:22-cv-00481 (D.D.C. Mar. 9, 2022), ECF 28 at 10-11.

Apple’s proposal allows virtually unlimited access to Confidential Information to any officer, director or employee to whom it alone thinks “such disclosure is reasonably necessary,” failing to put in place any guardrails and without consideration for competitive harm that would arise from sharing non-parties’ confidential research or commercial information directly with Apple’s business decision-makers. Apple has not shown prejudice, let alone how such prejudice outweighs the substantial risk of harm to non-parties.

3. Data Security (PPO § L.37-42)

Apple proposes to impose extensive data security and breach response obligations that, to Plaintiffs’ knowledge, have never been imposed on the Department of Justice or State Attorneys General in antitrust litigation. Apple proposes, among other things, that the United States and Plaintiff States “implement an information security management system . . . which shall comply with at least one of the then-current versions” of several standards applicable mainly to non-governmental entities. Ex. B ¶ 37. If a data breach potentially affects protected materials, Apple would require written notification within 48 hours, require the Parties to meet and confer over additional security measures, and require collateral discovery into any potential data breach. Apple also proposes that a data breach may require a stay or extension of litigation discovery while any data breach is investigated. Ex. B ¶ 40. Because these provisions appear in its Proposed Protective Order, Apple’s proposal necessarily would require the Court to police Plaintiffs’ compliance with data security and data breach protocols.

Apple’s proposal is neither workable nor necessary. As governmental entities, Plaintiffs are bound by specific and varied laws and policies governing data security and breach response. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to implement, maintain, and document information security programs, including establishing security controls, conducting security assessments, and reporting security incidents and breaches in accordance with established protocols. The Department of Justice also complies with the cybersecurity and privacy standards in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, with deviations or Plans of Action and Milestones and risk acceptance managed through applicable DOJ policies and procedures.

The States are bound by laws and policies governing data security and data breach obligations. New Jersey, for example, follows the New Jersey Statewide Information Security Manual, which requires all State information systems and services to implement, at a minimum, Moderate level controls in accordance with NIST SP 800-53 Revision 5. New York’s Information Security Policy No:NYS-P03-002 provides a robust framework of policies and procedures agencies must follow to ensure the physical and digital security of information. State laws govern and establish incident and breach reporting obligations and include, for example, New Jersey’s Identity Theft Prevention Act (ITPA), N.J.S.A. 56:8-161 to 56:8-166; California Civil Code § 1798.29; the Minnesota Government Data Practices Act, Minn. Stat. § 13.01 *et seq.*; and New York’s NYS Technology Law § 208.

Government bodies make legislative and administrative judgments about how to implement laws and policies to best suit their needs and the needs of their constituents. It would be impractical and disruptive to override Plaintiffs' authority as sovereign governments to instead impose a standard of Apple's choosing.

Plaintiffs acknowledge they will comply with applicable laws and policies that establish the framework under which the Department of Justice and State Attorneys General will maintain data security and respond to an incident or breach. Ex. A ¶ 34. National security and law enforcement equities may prohibit the Department of Justice from notifying affected persons within a certain time frame and disclosing certain information regarding a breach, as Apple proposes. The Department of Justice also cannot disclose sensitive information regarding government information systems, including any vulnerabilities that may have involved a breach. This Protective Order should not impose requirements that could be inconsistent with applicable federal or state laws or policies or potentially jeopardize national security, law enforcement, and other government equities.

The only case Apple cites in which the government was subject to additional data security protections is *United States v. Anthem, Inc.*, 2024 WL 2982908, at *1-2 (S.D.N.Y. June 12, 2024), but there the government agency was planning to host discovery data through a bespoke system for the litigation, and the agency's only objection was that the cost of additional security protections was not justified. Apple's remaining cases are class actions and private disputes that are not informative on the appropriate provisions for a data breach in this government enforcement action. *See, e.g., Floyd v. Amazon.com, Inc.*, 2023 WL 8701667 (W.D. Wash. Dec. 15, 2023). In recent private antitrust cases, Apple has also stipulated to protective orders that do not contain the invasive data security and incident or breach response obligations Apple demands here. *AliveCor, Inc. v. Apple Inc.*, 4:21-cv-03958 (N.D. Cal. Sep. 9, 2022), ECF 93; *Saurikit, LLC v. Apple Inc.*, 4:20-cv-08733 (N.D. Cal. June 24, 2021), ECF 53; *Cameron v. Apple, Inc.*, 4:11-cv-06714 (N.D. Cal. Jan. 21, 2021), ECF 381; *Epic Games, Inc. v. Apple, Inc.*, 4:20-cv-05640 (N.D. Cal. Oct. 1, 2020), ECF 110.

B. Defendant's Position

Plaintiffs' single-tier confidentiality proposal and limitations on disclosure are unduly burdensome, a deviation from typical practice in this District, depart from the approach the DOJ has agreed to and apparently found workable in other technology antitrust cases of similar size and complexity, impose prejudicial restrictions on Apple's litigation strategy, and carry a substantial risk of over-designation. Under Plaintiffs approach, documents would be subject to only a single designation of "Confidential" that operates in practice akin to an "attorneys' eyes only" provision. This single tier would permit only a narrow subset of four in-house counsel to review *any* documents designated Confidential regardless of the degree of sensitivity of the information. Plaintiffs brought this litigation, which Apple must now defend. Plaintiffs cannot now seek to artificially hamstring Apple's defense by foreclosing meaningful engagement and review of key documents by the Apple employees and in-house counsel most knowledgeable about Apple's business. Of course, such disclosures should be subject to reasonable limits, which Apple's proposed two-tier approach provides. Having two tiers of confidentiality, each with tailored

categories for access provides flexibility in terms of who can access what materials depending on their sensitivity.

1. Confidentiality Designation Tiers⁷

For over four months, Plaintiffs agreed with Apple's position and negotiated a protective order that included two tiers of confidentiality: (i) Confidential; and (ii) Highly Confidential – Attorneys Eyes Only. This approach is consistent with this District's Model Discovery Confidentiality Order, *see* NJ R UDSCT App. S ("Model"), and the designations used during the Government's investigation of Apple. In the eleventh hour of negotiations, Plaintiffs abruptly insisted on a single confidentiality tier without further discussion the day before the Parties were set to exchange final positions.

Two-tier protective orders are appropriate when heightened protection is necessary for particularly sensitive business information. As reflected in the Model, the baseline "Confidential" tier encompasses categories of lower-level proprietary information, whereas the "Highly Confidential – Attorneys Eyes Only" tier further restricts access to highly sensitive and competitive business information. Model at ¶¶ 1-2.

In the context of technology antitrust cases, courts routinely allow two-tiered designations and heightened protection for information such as competitively sensitive trade secrets, development and planning for future products, technical details concerning proprietary technology, and information regarding internal business strategy. *See, e.g., FTC v. Amazon.com, Inc.*, No. 2:23-cv-01495-JHC, Dkt. 160 (W.D. Wash. Feb. 13, 2024); *United States v. Google LLC*, No. 1:23-cv-00108-LMB-JFA, Dkt. 203 (E.D. Va. May 11, 2023).

Plaintiffs' single-tier approach is unjustified and unfairly prejudices Apple. For example, without two tiers of confidentiality, the multitude of third parties that will produce documents in this case will in all likelihood designate all materials as Confidential, which, under Plaintiffs' proposal, would greatly restrict the individuals who could review that information. That approach would impose significant limitations on who at Apple can view *any* third-party materials, regardless of whether they are competitively sensitive, negatively impacting Apple's ability to consult with its lawyers and prepare its defense. Contrary to Plaintiffs' position, and discussed more fully below, Apple does not seek unfettered access for its employees or in-house counsel to either tier of information. Each tier includes safeguards tailored to the sensitivity of the information.

Apple requests that the Court adopt its two-tiered proposal, which is the standard in this jurisdiction and consistent with other recent antitrust tech cases and the Parties' practice during the investigation.

⁷ *See* Ex. B §§ A.2(b), (f), ¶ 22.

2. Access to Confidential Materials⁸

Under the two-tiered approach to which the Parties originally agreed, Plaintiffs seek to prohibit all Apple officers, directors, or employees—and all but four Apple in-house counsel—from accessing the vast majority of materials likely to be used by the Government in prosecuting its case. Plaintiffs’ position is untenable.

Forbidding all but four Apple in-house counsel from reviewing any Confidential materials is highly prejudicial and would prevent essential Apple employees and in-house counsel from assisting in the company’s defense against a case attacking a broad swath of products, services, and design decisions. Indeed, Plaintiffs’ own cited case recognizes that “[t]o deny outside counsel access to the lawyers most familiar with their clients’ business ... and who will have a much deeper and complete understanding of the documents being produced ... is to make [defendants] fight with one hand behind their backs.” *United States v. Sungard Data Sys., Inc.*, 173 F. Supp. 2d 20, 21 (D.D.C. 2001). What’s true for in-house counsel applies also to Apple employees, whose technical knowledge and expertise are needed by outside counsel to evaluate Plaintiffs’ claims implicating Apple’s advanced, proprietary technology. *See Motorola, Inc. v. Lemko Corp.*, 2010 WL 2179170, at *5 (N.D. Ill. June 1, 2010) (recognizing “legitimate need for ... outside counsel to be able to consult with client representatives other than lawyers”).

As such, Apple proposes that employees and counsel be allowed to view Confidential materials, with key limitations preventing unfettered access. Specifically, Apple proposes that Confidential materials may only be disclosed to Apple officers, directors, employees, and in-house counsel, as well as their immediate staff, where such disclosure is ***reasonably necessary*** for this Action, and provided that ***each individual agrees to be bound by the Protective Order***. Even tighter access limitations would apply to Highly Confidential materials.⁹

The Model and precedent support Apple’s position. The Model allows disclosure of Confidential materials to relevant in-house counsel and the parties’ representatives where such disclosure is “necessary” to the litigation. *See* Model at ¶ 4(g). Similarly, in *United States v. Google LLC*, the protective order permits disclosure of confidential information to “the officers, directors, and employees (including In-House Counsel) of Defendant to whom disclosure is reasonably necessary for this litigation.” No. 1:23-cv-00108-LMB-JFA, Dkt. 203 at 20 (E.D. Va. May 11, 2023). *See also Motorola, Inc. v. Lemko Corp.*, No. 1:08-cv-05427, Dkt. 96 at 5-6 (N.D. Ill. Apr. 3, 2009) (allowing disclosure of Confidential information to employees “required in good faith to provide assistance”); *In re Lantus Direct Purchaser Antitrust Litig.*, No. 1:16-cv-12652, Dkt. 98 at 12 (D. Mass Apr. 27, 2020) (similar).

⁸ Ex. B ¶ 21.

⁹ Specifically, unless they are a witness or deponent who the Receiving Party has “a good faith belief” authored or received the document or had involvement or responsibilities regarding the subject matter, Apple employees would not have access to Highly Confidential materials under Apple’s proposal. Additionally, in-house counsel access is limited to four individuals not involved in business decisions.

Plaintiffs' own cases recognize the importance of allowing at least in-house counsel access to confidential information where necessary. *See Sungard*, 173 F. Supp. 2d at 21. And Plaintiffs have not demonstrated how disclosure of Confidential information to in-house attorneys whose responsibilities are largely "legal and security-related" would pose a risk of spillage when all "will be subject to non-disclosure / non-use restrictions under the Court's protective order." *Motorola*, 2010 WL 2179170, at *4.

The Court should adopt the access proposal outlined in Apple's approach, which allows certain necessary Apple employees and in-house counsel (as well as outside counsel for Apple and counsel for Plaintiffs) to access Confidential materials, and limits Highly Confidential materials to just outside counsel and a limited number of Apple in-house attorneys.¹⁰

3. Data Security¹¹

Apple's proposal includes industry-standard data security provisions to protect against unauthorized access to sensitive data and mitigate risk after a data breach. Plaintiffs claim they only can agree to comply with a vague reference to "applicable security, privacy, data protection, and breach response and notification laws, rules, regulations, policies, and directives"¹² and refuse to agree to Apple's proposed security provisions without articulating why such provisions are burdensome or prejudicial. Data breaches pose significant threats, and Apple's proposed measures aim to safeguard all materials disclosed in this action, including those produced by non-parties.

Data security is at the core of Apple's business. Apple prioritizes the protection of users' data, partners' business data, and its own trade secrets, business strategy, and financial information. Discovery in this case will likely implicate and involve production from all these categories, for both Apple and third parties. Data security, moreover, is a significant concern with real-world implications. For example, organized criminal groups and hostile state actors perpetrate data security attacks with growing frequency. Data breaches have increased year-over-year, including a striking 20% jump from 2022 to 2023.¹³ Indeed, 2024 "is on pace to be the biggest year in the history of law firm data breach reports" with 21 law firms filing breach reports to state attorneys general offices in the first five months.¹⁴ And the government is not immune from data breaches. A White House report indicated that in 2023, federal agencies suffered 11 "major" data security incidents and that the Department of Justice itself reported "multiple incidents," including

¹¹ Ex. B § L.

¹² Ex. A § L.

¹³ *See* Stuart Madnick, *Why Data Breaches Spiked in 2023*, HARVARD BUS. REV., Feb. 19, 2024, available at, <https://hbr.org/2024/02/why-data-breaches-spiked-in-2023> (last visited on Sept. 12, 2024).

¹⁴ Dan Roe, *Law Firm Data Breach Reports Show No Signs of Slowing in 2024*, AM. LAWYER, May 23, 2024, available at <https://www.law.com/americanlawyer/2024/05/23/law-firm-data-breach-reports-show-no-signs-of-slowing-in-2024/?sreturn=20240816121021> (last visited Sept. 16, 2024).

one that impacted “case-specific data analytics support for the Civil Division and several United States Attorneys’ Offices.”¹⁵ The federal judiciary has also recognized the need to implement additional safeguards for court records due to “recent disclosure of widespread cybersecurity breaches of both private sector and government computer systems....”¹⁶

In light of this mounting threat,¹⁷ Apple’s proposed data security protections are common sense and necessary. Courts have approved protective orders including provisions consistent with the protections Apple seeks.¹⁸ See, e.g., *In re Insulin Pricing Litig.*, No. 17-699, Dkt. 299 at 12 (D.N.J. Jan. 23, 2020) (“Protected Material...shall be maintained in secure litigation support site(s) that applies standard industry practices regarding data security.”); *Park v. Sam’s East, Inc.*, No. 20-cv-03119, Dkt. 46 § 6 (D.N.J. Sept. 23, 2021) (requiring “secure data storage systems, established security policies, and security training for employees, contractors and experts,” as well as “data encryption ..., data access controls, and physical security”); *Apple Inc. v. Rivos, Inc.*, No. 5:22-cv-2637, Dkt. 113 at 14 (N.D. Cal. Oct. 31, 2022) (requiring parties to implement an information security management system that complies with an industry or government cybersecurity framework, encrypt materials in transit, implement MFA, and follow certain procedures in response to a data breach); *Sheet Metal Workers’ Nat’l Pension Fund v. Bayer Aktiengesellschaft*, No. 3:20-cv-04737, Dkt. 138 at 19-20 (N.D. Cal. Oct. 6, 2022) (requiring storage in a site or source that applies “standard industry practices regarding data security,” among other measures); *Anderson v. Gen. Motors, LLC*, Case No., 2:22-cv-00353, Dkt. 38 at 8 (E.D. Cal. Sept. 6, 2022) (similar).

In *Floyd v. Amazon.com, Inc.*, the court ordered data security protections nearly identical to those Apple proposes here. 2023 WL 8701667, at * 1-3 (W.D. Wash. Dec. 15, 2023). The court required plaintiff to “implement data management systems complying with established data security frameworks” and MFA. *Id.* Moreover, it adopted a list of reasonable remedial actions to be taken in the event of a data breach, similar to the actions proposed here. *Id.* The *Floyd* court reasoned that defendants’ proposed “commonplace” security measures appropriately safeguarded

¹⁵ Federal Information Security Modernization Act of 2014 Annual Report Fiscal Year 2023, pp. 20, 22, available at <https://www.whitehouse.gov/wp-content/uploads/2024/06/FY23-FISMA-Report.pdf> (last visited Sept. 12, 2024).

¹⁶ <https://www.uscourts.gov/news/2021/01/06/judiciary-addresses-cybersecurity-breach-extra-safeguards-protect-sensitive-court> (articulating the need for additional security measures and quoting James C. Duff, Secretary of the Judicial Conference of the United States, stating “The federal Judiciary’s foremost concern must be the integrity of and public trust in the operation and administration of its courts. . .”).

¹⁷ Robert Hilson, *Why the archaic process for eDiscovery is vulnerable to hacking and data breach*, Logikcull (Feb. 8, 2017), <https://www.logikcull.com/blog/archaic-process-e-discovery-vulnerable-hacking-data-breach#:~:text=It's%20an%20incredibly%20risky%20process,channels%20expose%20information%20to%20breach> (last visited on Sept. 12, 2024).

¹⁸ Plaintiffs note that the Model does not yet include a data security provision. This is unsurprising and not dispositive given the technically complex and rapidly evolving nature of cybersecurity risks and corresponding safeguards. Courts are issuing data security orders with more frequency.

confidential material without unduly burdening the plaintiff or third parties. *Id.* at *1, 3. The court noted that defendants’ proposals for managing a potential data breach were not “burdensome or unworkable,” but rather allowed flexibility to “craft an appropriate response based on the particular circumstances of a data breach.” *Id.* at *2.

Apple proposes the implementation of security measures complying with a recognized cybersecurity framework, such as that of the Center for Internet Security or another well-recognized industry or government cybersecurity framework. These are frameworks with which many vendors and companies already comply, and any burden is minimal. Plaintiffs’ refusal to stipulate to these minimum standards is concerning and unwarranted.

To mitigate the risk of unauthorized access, Apple also proposes encryption of produced materials and implementation of multi-factor authentication (“MFA”), measures regularly used in data security practice. MFA has been called the “single most important thing Americans can do to stay safe online,” and is a simple, highly effective security mechanism.¹⁹ In fact, the federal judiciary recently requested funding to implement enterprise-wide MFA.²⁰

Additionally, Apple’s proposal facilitates prompt mitigation and remediation of a data breach, including notifying the producing party and providing steps to mitigate the breach. Apple’s proposal requires that the receiving party comply with the producing party’s reasonable requests to investigate, remediate, and mitigate the effects of the breach, provide information that is reasonably requested and relates to the breach, and meet and confer regarding any necessary adjustments. In contrast to Plaintiffs’ mere agreement to comply with the law, these provisions set clear expectations on basic steps for investigation after a breach. None of these provisions imposes significant burdens, and taken together, they provide strong protections from real and serious data security threats.

Notably, the government has been required to implement more stringent security measures than what Apple proposes here. *See, e.g., United States v. Anthem, Inc.*, 2024 WL 2982908, *3 (S.D.N.Y. June 12, 2024) (requiring the government implement “robust” protections). In *Anthem*, the government agreed to, among other things: house data on a bespoke platform, not connected to the internet; transfer data via encrypted physical storage; and implement a HITRUST-certified security system. *Id.* The court further required that the government add additional cybersecurity protections, including tracking and logging activity on the platform and adopting data loss prevention controls. *Id.*

To the extent Plaintiffs expect Apple to take it on faith that current laws or policies—whatever those may be—mandate sufficient protection for produced data, that is insufficient. In recent years, both federal and state governments have failed to adequately protect data produced in litigation or otherwise. *See, e.g., Anthem*, 2024 WL 2982908, at *3 (noting that “given the

¹⁹ Jen Easterly, *Next Level MFA: FIDO Authentication*, Cybersecurity & Infrastructure Security Agency, Oct. 18, 2022, <https://www.cisa.gov/news-events/news/next-level-mfa-fido-authentication> (last visited Sept. 12, 2024).

²⁰ *See The Judiciary Fiscal Year 2023 Congressional Budget Request: Judiciary Information Technology Fund*, The Administration Office of the U.S. Courts (Mar. 2022).

previous breach [by the government’s vendor], Anthem’s concern for the security of the data is reasonable”); Notice of Data Breach, Rob Bonta, Cal. Off. Atty. Gen. (July 8, 2022) (notifying citizens that their personal information was disclosed by the California Department of Justice).

In light of these risks, Apple and this Court “can not [sic] rely on the representations of lawyers for the government to conclude that their proposed safeguards are sufficient.” *Anthem*, 2024 WL 2982908, at *4. Apple proposes reasonable protections and remedial procedures consistent with widely recognized data security standards of care and protective orders in recent cases, and asks that the Court adopt its proposal.

III. ESI PROTOCOL

A. Plaintiffs’ Position (ESI § IV.10)

Plaintiffs’ ESI Protocol requires a Producing Party to provide metadata for relevant linked documents from communications within the production. It appropriately requires the Producing Party to provide this information. Under Apple’s proposal, no information about linked documents is provided unless requested. Apple requires that the Requesting Party ask for any information about specific linked documents—inverting standard discovery burdens. Plaintiffs’ proposal incorporates Apple’s proposal, but also requires a Producing Party to provide metadata about relevant linked files in the first instance, instead of requiring the Requesting Party to seek additional information about specific documents after production occurs.

Apple contends Plaintiffs’ separate proposal (“Plaintiffs’ Proposal”) is unduly burdensome without engaging with it. Apple has never responded to multiple, repeated requests for information about its concerns with Plaintiffs’ Proposal.²¹ It has not shared simple information that could allow the parties to collaborate or compromise. Contrary to Apple’s contentions, nothing in Plaintiffs’ Proposal requires collection of documents from a Party’s files and servers. Yet Apple’s cases and position suggest it does. Apple offers only the cursory conclusion that Plaintiffs’ Proposal is manual and therefore burdensome. That is inadequate. “A party resisting discovery on the grounds of burden or expense bears the burden of showing specifically how the request is burdensome.” *IQVIA, INC. v. Veeva Sys., Inc.*, 2019 WL 3069203, at *5 (D.N.J. July 11, 2019) (requiring linking of documents). Apple fails to make this showing.

1. Linked Documents Are Critical to Business Today

Linked documents (such as iCloud.com or Box.com files) are collaborative files that enable people to work together on a document. Linked documents are critical to contemporary business. Often, the most important documents in a company are not created by an individual contributor, but reflect collaboration and input from many people and potentially many teams. The most important documents are often linked documents.

This is especially true for Apple. Apple employees routinely transmit and share linked documents. There are hyperlinks to tens of thousands of collaborative documents in Apple’s pre-

²¹ Plaintiffs’ Letter to Alexia Brancato (Sept. 14, 2024) (“Sept. Letter”).

Complaint productions. Apple appears to handle entire projects on collaborative platforms, and relevant Apple communications link to files in collaborative platforms, such as Quip.com, iCloud.com, and Slack.com.

Apple does not dispute that its linked documents contain relevant information and are important to its business.

2. Plaintiffs' Proposal Is Narrowly Drawn

Plaintiffs' Proposal recognizes the importance of linked documents but is crafted to reduce the burdens on a Producing Party by requiring reasonable and limited productions. For example:

- Plaintiffs' Proposal does not require production of any additional linked documents that are not already identified for production. It only requires production of metadata to enable cross-referencing of relevant linked documents in the production.
- Plaintiffs' Proposal does not apply to all linked documents that are identified, preserved, or collected. It only applies to linked documents within the production, i.e., relevant, responsive documents.
- Even then, Plaintiffs' Proposal does not require hyperlink metadata for all linked documents within the production. It only requires metadata for linked documents in the production where the hyperlink also appears relevant based on the face of the communication.

These significant limits are intended to ensure that the value of the linked document information is high and the burden is proportionate and tailored to the needs of the case.

3. Plaintiffs' Proposal Is Reasonable and Proportional

Plaintiffs' Proposal only requests metadata for relevant linked documents from communications within the production—without requesting the documents themselves. The proposal itself builds in significant limits and proportionality analysis.

The proportionality factors favor Plaintiffs' Proposal. Rule 26(b)(1) proportionality assesses the “importance of the issues at stake.” Here, this landmark antitrust action raises issues of national importance for consumers nationwide. *See, e.g., Lawlor v. Nat'l Screen Serv. Corp.*, 349 U.S. 322, 329 (1955) (recognizing “the public interest in vigilant enforcement of the antitrust laws”); FED.R.CIV.P. 26 advisory committee’s note (recognizing the importance of “cases in public policy spheres” and injunctive cases “that seek[] to vindicate vitally important personal or public values”).

The “parties’ resources” favor Plaintiffs' Proposal. FED.R.CIV.P. 26(b)(1). Apple is a sophisticated technology company and one of the largest publicly traded companies in the world. There is no doubt that Apple, the company that created some of these communication and

collaboration platforms (like iCloud, iMessages, and Apple Mail), can comply with its discovery obligations by producing linked document metadata. Apple’s vast monetary resources and unique technology expertise are features in the proportionality analysis.²² Any solutions Apple implements to automatically pull linked document metadata in this case would benefit Apple’s other cases—and any cost to Apple for doing so should be amortized across Apple’s docket of thousands of cases from the past decade.

4. Apple Fails to Show Undue Burden

Apple protests that Plaintiffs’ Proposal is unduly burdensome because it is not automatic. But access to an automatic tool is not the end of the inquiry. Like any sophisticated, repeat litigant, Apple cannot fail to invest in necessary tools for modern eDiscovery and then evade compliance by claiming that the process is unduly burdensome without those tools.

Sophisticated parties regularly produce linked documents. For example, Google recently agreed to produce all links from its emails to collaborative documents on its proprietary collaborative platforms, and Ticketmaster and Live Nation agreed to produce linked documents and metadata in OneDrive, SharePoint, and Teams. *See* Letter Agreement, *United States v. Google*, 1:20-cv-03010 (D.D.C. Jan. 15, 2021); Order Governing ESI Discovery, ECF 249 at 12, *United States v. Live Nation*, 1:24-cv-03973 (S.D.N.Y. Aug. 28, 2024).

Plaintiffs did not seek all linked documents here because Apple represented this would not be feasible. While Plaintiffs are not aware of identical ESI protocols, other courts have largely rejected far broader requests for linked documents, without the tailoring evident here.²³ Cases involving far broader proposals say little about Plaintiffs’ carefully crafted proposal.

To establish undue burden, Apple must offer specifics that it has not provided. “The application of proportionality should be based on information rather than speculation.”²⁴ “Burden and expense should be supported by hard information and not by unsupported assertions.”²⁵ But Apple has not responded to Plaintiffs’ repeated requests for information about its concerns with Plaintiffs’ Proposal.²⁶ Apple has not provided basic information, such as what processing and

²² *See* The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 Sedona Conf. J. 141, 172 (2017) (“Sedona, *Proportionality*”).

²³ *See In re Insulin Pricing Litig.*, 2024 WL 2808083, at *7-8 (D.N.J. May 28, 2024) (plaintiffs sought “family-complete” linked documents, requiring collection of *all* linked documents, regardless of relevance or value); *Nichols v. Noom, Inc.*, 2021 WL 948646 (S.D.N.Y. Mar. 11, 2021) (plaintiffs sought *all* linked documents regardless of relevance or value); *see In re StubHub Refund Litig.*, 2024 WL 2305604, at *1-3 (N.D. Cal. May 20, 2024) (defendants identified and matched collected documents to their hyperlinks already).

²⁴ Sedona, *Proportionality* 162 (Principle 4).

²⁵ *Id.* at 167; *see* FED.R.CIV.P. 34(b)(2)(B) (responding party must “state with specificity the grounds for objecting to the request, including the reasons”).

²⁶ Sept. Letter.

review tools it will use or where hyperlinks are stored on Apple's collaborative platforms.²⁷ Missing information like this is critical to Apple's claims of burden and technical infeasibility.

Apple's primary, disingenuous argument is that it lacks an automated tool to accomplish Plaintiffs' Proposal. But simple eDiscovery tools can automatically extract hyperlinks, and those tools can be configured to extract hyperlinks from only specific platforms (like box.com) or with specific text (like document IDs).²⁸ Similarly, matching metadata is common and straightforward in any large-scale litigation. Matching hyperlinks in communications with their shared documents involves matching metadata. eDiscovery service providers and in-house discovery teams regularly and automatically match metadata of all kinds. And collaborative platforms—like box.com—can store and export shared links for all collaborative documents.²⁹

Apple has multiple, feasible options to fulfill its discovery obligations under Plaintiffs' Proposal, and it has failed to establish otherwise.

B. Defendant's Position

1. Production of Linked Files and Collaborative Work Environments³⁰

The Parties dispute the proper way to handle producing hyperlinks contained in responsive documents. Apple's proposal allows for the receiving party to make reasonable requests for the producing party to identify and, if found, produce hyperlinks contained in produced documents. While Plaintiffs seemingly have agreed to Apple's compromise to search for requested documents, Plaintiffs insist that in addition the Parties must identify *all* corresponding hyperlinks within produced documents and provide metadata and logs for those files. The Court should adopt Apple's proposal because there is no automated process to collect and associate documents or hyperlinks in the way Plaintiffs request.

Unpacking Plaintiffs' proposal reveals just how burdensome it is. In the absence of an automated tool, their suggested process requires that during pre-production review of documents the parties: (1) manually identify all hyperlinks in documents that are to be produced; (2) evaluate each hyperlink within the document to determine whether it links to another document; (3) make a determination whether the linked document is potentially relevant; (4) manually populate a metadata field with each hyperlink address for a document determined to be potentially relevant; (5) conduct a manual search to see if the documents corresponding to those hyperlinks are also in the production universe; and (6) manually populate a metadata field with a corresponding bates

²⁷ *Id.*

²⁸ For example, regular expression ("Regex") searches enable parties to automatically extract hyperlinks. Regex searches are tools commonly available in eDiscovery platforms, and parties commonly use Regex searches to identify PII for potential redactions.

²⁹ *See, e.g.*, Box.com Shared Link Report, <https://support.box.com/hc/en-us/articles/4415098138899-Shared-Links-Report> (last updated June 25, 2024).

³⁰ Ex. C § V.10.

number if the document was produced; or (7) for documents not produced, create a log of the hyperlinked addresses. This is unduly burdensome.

In contrast, Apple's common-sense proposal allows for the receiving party to identify hyperlinks contained in produced documents and make reasonable requests for the producing party to search for a corresponding relevant link and, if found, produce that document.

The Court should adopt Apple's proposal because Apple does not have an automated tool capable of implementing Plaintiffs' proposal and to Apple's knowledge no such off-the-shelf tool exists in the market. Courts have found that "hyperlinks are not the same as traditional attachments." *In re Insulin Pricing Litig.*, 2024 WL 2808083, at *7 (D.N.J. May 28, 2024); *see also Nichols v. Noom Inc.*, 2021 WL 948646, at *4 (S.D.N.Y. Mar. 11, 2021) (noting that hyperlinks are not the same as attachments). Because hyperlinks are not attachments, collecting, processing, reviewing, or producing them as "family" members with the documents in which they are transmitted is not technologically feasible absent an automated tool.

In the absence of automated tools, courts have adopted approaches similar to Apple's proposal, where the parties make reasonable requests to search for and produce hyperlinked documents. Like Apple, the defendants in *In re Insulin* also did not have an automated tool and thus objected to the plaintiff's proposal to search, collect, associate, and produce hyperlinks. 2024 WL 2808083, at *7. The court agreed with defendants and found that because defendants' "tools are either not feasible whatsoever or unduly burdensome to apply to their respective data environments" the defendants were not required to collect hyperlinks. *Id.*; *see also In re StubHub Refund Litig.*, 2024 WL 2305604, at *1 (N.D. Cal. May 20, 2024) (removing requirement that hyperlinked documents be produced in document family groups when there is no automated tool); *In re Meta Pixel Healthcare Litig.*, 2023 WL 4361131, at *1 (N.D. Cal. June 2, 2023) (finding "parties should consider reasonable requests for production for hyperlinked documents on a case-by-case basis. Such requests should not be made as a matter of routine"); *Nichols*, 2021 WL 948646, at *1 (noting that defendant "has already agreed to produce a reasonable number of linked documents at Plaintiffs' request" and refusing to require defendant to collect all hyperlinks).

Notably, the government recently agreed to provisions substantially similar to Apple's proposal in other recent antitrust litigations. *See e.g., United States v. Google LLC*, No. 1:23-cv-00108-LMB, Dkt. 142 at 26 (E.D. Va. Apr. 20, 2023) (stipulating to language nearly identical to Apple's proposal); *see also Texas v. Google LLC*, No. 4:20-cv-00957-SDJ, Dkt. 183 at 24 (E.D. Tex. Dec. 13, 2023) (same). Instead of similarly agreeing to a straight-forward approach here, Plaintiffs insist upon requiring Apple to manually search for and provide additional information on top of what Apple has already agreed to provide.

Plaintiffs' proposal is unduly burdensome and inefficient. Plaintiffs' proposal will significantly disrupt and delay Apple's workflow for processing, review, and production of documents. Creating this manual workflow will only serve to complicate an already complex review and slow down Apple's ability to review and produce documents. Courts frequently refuse to impose this kind of burden. *See In re Meta Pixel*, 2023 WL 4361131, at *1 (refusing to require defendants to use a tool or process that would "disrupt [its] standardized workflow for ESI-related discovery processing across all of its platforms and systems," and holding the "ESI protocol should

make clear that hyperlinked documents are not treated as conventional attachments....”); *In re StubHub Refund Litig.*, 2024 WL 2305604, at *2 (finding that the “non-existence of commercially available software that can implement the hyperlink requirement tips strongly” in removing the requirement to collect hyperlinks).

Curiously, Plaintiffs argue that Apple must divert money and resources from its business and enter the eDiscovery space to develop tools to assist litigants with collecting and producing hyperlinks. Plaintiffs cite no authority for such a bold assertion. It is well settled that parties need only produce documents as they are stored in the “usual course of business,” and courts do not require parties to invent new technology to respond to discovery requests and make unduly burdensome requests less burdensome. Fed. R. Civ. P. 34(b)(2)(E)(i); *see Nichols*, 2021 WL 948646, at *4 (rejecting plaintiffs’ proposal that would require defendant’s programmers to develop a tool to search and associate hyperlinks).

The one case on which Plaintiffs rely supports Apple’s proposal.³¹ In *United States v. LiveNation*, the parties agreed that “to the extent reasonably feasible and capable of being done automatically, the producing party shall use its best efforts using available technical solutions to produce the document corresponding with each identified link.” No. 1:24-cv-03973, at 12 (S.D.N.Y. Aug. 28, 2024) (emphasis added).³² As Apple has repeatedly explained, Plaintiffs’ proposal is not reasonably feasible nor capable of being done automatically.

Finally, Plaintiffs mischaracterize Apple’s proposal as somehow attempting to evade its discovery obligations. This is false. Apple has never indicated that it would not search, collect, or produce responsive information from appropriate data sources. Given current technical limitations, Apple, like many companies, simply cannot pair the pointer email or messages and hyperlinked documents on the back end.

³¹ Plaintiffs cite a Letter Agreement in *United States v. Google LLC*, No. 1:20-cv-03010-APM (D.D.C. Jan. 15, 2021), but Apple was unable to locate this letter on the docket and, regardless, the ESI Protocol filed in that matter did not provide for the production of hyperlink files. *See United States v. Google LLC*, No. 1:20-cv-03010-APM, Dkt. 99 (D.D.C. Jan. 21, 2021). Moreover, Plaintiffs explain that Google agreed to produce hyperlinks for OneDrive, SharePoint, and Teams, which are part of Microsoft’s suite and may have an automatic tool to connect links to their messages.

³² The protocol in *LiveNation* also states that “[t]o the extent reasonably feasible and capable of being done automatically, for each Linked Attachment, the producing party will use available technical solutions to attempt to populate the LINKEDPARENTIDS field with the document control numbers ... [and] the producing party will employ commercially reasonable efforts to provide an overlay file populating these two fields ... to the extent feasible with available technical solutions.” *LiveNation*, No. 1:24-cv-03973, at 12 (emphasis added).

Respectfully submitted,

/s/ Jonathan H. Lasken

Jonathan H. Lasken
Assistant Chief, Civil Conduct Task Force
United States Department of Justice
450 Fifth Street, NW, Suite 4000
Washington, D.C. 20530
Telephone: (202) 598-6517
Email: jonathan.lasken@usdoj.gov

PHILIP R. SELLINGER
United States Attorney

/s/ J. Andrew Ruymann

J. Andrew Ruymann
Assistant United States Attorney
U.S. Attorney's Office
402 East State Street, Room 430
Trenton, NJ 08608
Telephone: (609) 989-0563
Email: John.Ruymann@usdoj.gov

MATTHEW J. PLATKIN
Attorney General of New Jersey

/s/ Isabella R. Pitt

Isabella R. Pitt (NJ Bar No. 071002013)
Deputy Attorney General
Assistant Section Chief of Antitrust
New Jersey Office of the Attorney General
124 Halsey Street, 5th Floor
Newark, NJ 07101
Telephone: (973) 648-3070
Isabella.Pitt@law.njoag.gov

*Attorney for Plaintiff State of New Jersey,
Arizona, California, Washington D.C.,
Connecticut, Indiana, Maine,
Massachusetts, Michigan, Minnesota,
Nevada, New Hampshire, New York, North
Dakota, Oklahoma, Oregon, Tennessee,
Vermont, Washington, and Wisconsin*

/s/ Liza M. Walsh

Liza M. Walsh
Douglas E. Arpert
WALSH PIZZI O'REILLY FALANGA LLP
Three Gateway Center
100 Mulberry Street, 15th Floor
Newark, New Jersey 07102
Tel.: (973) 757-1100
Email: lwalsh@walsh.law
Email: darpert@walsh.law

/s/ Crais S. Primis

Craig S. Primis, P.C.
Winn Allen, P.C.
KIRKLAND & ELLIS LLP
1301 Pennsylvania Avenue, N.W.
Washington, DC 20004
Tel.: (202) 389-5000
Email: craig.primis@kirkland.com
Email: winn.allen@kirkland.com

/s/ Devora W. Allon

Devora W. Allon, P.C.
Alexia R. Brancato
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, NY 10022
Tel.: (212) 446-4800
Email: devora.allon@kirkland.com

Attorneys for Defendant Apple Inc.

PHILIP R. SELLINGER
United States Attorney

BY: JONATHAN LASKEN
Assistant Chief
Civil Conduct Task Force
United States Department of Justice
Antitrust Division
450 Fifth Street NW, Suite 8600
Washington, DC 20530
Attorney for Plaintiff United States of America

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA et al.,

Plaintiff,

v.

APPLE INC.

Defendants.

Case No. 2:24-cv-04055-JXN-LDW

CERTIFICATE OF SERVICE

I hereby certify that the above letter and this Certificate of Service were served upon defendant's counsel, Liza M. Walsh, Esq., Craig S. Primis, Esq., Devora W. Allon, Esq., and K. Winn Allen, Esq., 1301 Pennsylvania Avenue, NW, Washington, D.C., 20004, by CM/ECF on September 20, 2024.

BY: s/ Jonathan H. Lasken
Jonathan H. Lasken
Assistant Chief
Civil Conduct Task force
United States Department of Justice
Antitrust Division
Attorney for Plaintiff United States